

Mitratesch Curacao B.V. Information Security Policy

Table of Contents

1. Purpose and Scope.....	2
2. Applicability.....	3
3. Governance & responsibilities.....	4
4. Information Security Principles & controls.....	4
4.1 Principle 1 — Establish effective management oversight.....	4
4.2 Principle 2 — Design, implement and maintain an ISM framework.....	5
4.3 Principle 3 — Maintain ongoing risk assessment program.....	7
4.4 Principle 4 — Establish information security monitoring.....	7
4.5 Principle 5 — Incident management & response.....	8
4.6 Principle 6 — Privacy of customer information.....	9
4.7 Principle 7 — Information security training.....	10
4.8 Principle 8 — Audit the ISM process.....	10
5. Definitions.....	11
6. Policy maintenance & review.....	11

Document History

Version No.	Author	Creation Date	Approver	Approval Date	Change Summary
1.0	Billy-Jay Smith	23-10-2025	Board of Directors	xx-xx-xxxx	Policy Creation

1. Purpose and Scope

Mitratesh Curacao B.V. with the registration number 146806, and registered address Zuikertuintjeweg Z/N (Zuikertuin Tower), Curacao (the “Company” or “Mitratesh”) is a Curacao registered and licensed entity, in accordance with the provisional license number ID/U1444/25 granted to it by the Gaming Control Board (“GCB”) of Curacao (also known as the Curacao Gaming Authority “CGA”) to provide critical services or goods in or from Curacao as referred to in Article 5.13, paragraph 1 of the National Ordinance on Games of Chance (LOK).

As the CGA does not provide specific frameworks for Information Security Management, this policy has been tailored to implement the Centrale Bank van Curaçao en Sint Maarten’s **Provisions and Guidelines for Information Security Management (ISM Provisions)** and aligns with industry best practice (ISO 27001/27002, NIST concepts) while being tailored to the Company’s business model. It indicates where each Policy section maps to the Bank’s Principles and provides detailed explanations of how the company meets the requirements of each principle.

The Board and Senior Management of the Company are committed to protecting the confidentiality, integrity and availability of information assets that support our API aggregation platform, to meet regulatory obligations and to reduce legal and reputational risk in a cost-effective manner. This policy sets mandatory governance, risk management, operational and technical expectations to fulfil the ISM Principles issued by the Centrale Bank.

2. Applicability

This Policy applies to:

- All employees, contractors, consultants and long-term third parties.
- All systems, services, APIs, networks, infrastructure, code repositories, development and production environments used to deliver the aggregation service to clients (including cloud services and any outsourced components).
- All client data, provider (game vendor) data and internal corporate information that is created, received, stored, transmitted or destroyed by the company.

(Principle mapping: Principle 2 — ISM framework scope definition).

3. Governance & responsibilities

Board of Managing Directors / Executive Committee

- Approve this Policy and ensure resourcing and oversight of the ISM program.
- Receive at least annual ISM status reports and ad-hoc notifications for major incidents.

ISM Coordinator

- Maintain the ISM program, prioritize projects (risk-based), approve standards and monitor implementation.

Information Security Manager (ISM Owner)

- Day-to-day ownership, risk reporting, incident coordination, training program owner.

System Owners, Process Owners, HR, Procurement, Legal, Ops, Dev

- Defined responsibilities for asset ownership, access approval, supplier selection and contract security clauses.

4. Information Security Principles & controls

This section maps the Bank's eight ISM Principles into policy statements the Company enforces. Each sub-section includes the requirements at law and detailed explanations of the processes in place for the Company to comply with the requirements of each principle.

4.1 Principle 1 — Establish effective management oversight

Policy requirement: The Board/Senior Management will ensure ISM policies, standards and procedures exist, be formally approved, and are subject to independent review. KPIs/KGIs shall be defined and reported.

- The information Security Management framework is reviewed and updated in line with any applicable changes to the systems or frameworks used by the Company in

the delivery of its services. In the absence of any changes that would warrant an update to this framework, the documentation will be reviewed and updated at least annually.

- The Company's Senior Management will;
 - Approve and formally own the Information Security Management system of the Company
 - Allow sufficient resources to implement correct information security management.
 - Appoint an ISM Coordinator to oversee program delivery, prioritise projects and report progress to the board.
 - Ensure independent reviews of ISM activities. More information on the Company's audit plans can be found in chapter 4.8.
- KPIs for the Company materialise in the form of comprehensive log management for our API services. System up-time is defined as "the period of time a computer, server, or service is operational and available for use. It is a key metric for reliability and is often expressed as a percentage to indicate how much of a given period the system was functional, with a higher percentage meaning greater reliability." As the Company's services are hosted on AWS Infrastructure, system up time is continuously monitored above 99%.
-

4.2 Principle 2 — Design, implement and maintain an ISM framework

Policy requirement: Implement and maintain an ISM framework that includes documented policies, standards, procedures, technologies and organizational structures aligned to ISO 27002 control objectives (Asset Management, HR security, Physical security, Communications & Operations, Access Control, Secure development, Incident Management, BCM, Compliance, technical hardening).

- Secure system architecture and engineering principles are crucial for building secure systems throughout their development lifecycle. Industry best practises emphasize creating, documenting, and upholding principles for secure system development, integrating security into all layers of architecture, including business, data, applications, and technology. Key principles being applied by the Company include incorporating secure and tamper-resistant codebases and authentication mechanisms, and implementing secrets management best practices to safeguard sensitive data like API keys and passwords.
- Establishing secure baseline configurations is fundamental for information security, maximizing security, and minimizing unauthorized access. Mitratech configures its systems in line with industry consensus guidelines, ensuring optimum security from the moment a component or asset is introduced into the Company's systems. Additionally, initial setup and security configuration of new systems is performed in a secure, isolated environment.
- Asset Management and Data classification are core components of an Information Security management system. The Company has built and maintains a complete, up-to-date inventory of information assets (hardware, software, business applications, datasets, documents, roles/owner matrix). All information assets shall

be classified (e.g., Public / Internal / Confidential / Restricted) and handling requirements assigned. The classification scheme and owners shall be reviewed annually or as required after a material change.

- All employees ensure secure document handling, e-mail controls, and archival/destruction of records consistent with the Company retention schedule. Sensitive records are stored and transmitted in encrypted form and access logged to these records are logged accordingly.
- A change management process is essential to maintain information security during system modifications. Changes are categorized and assessed for security and operational impact. A structured workflow for authorizations, rollback plans, and stakeholder notifications is in place to ensure any implemented change follows secure configuration management, ensuring systems are deployed and maintained with hardened defaults and secure baselines, and that these configurations are preserved during system updates.
- Patch management is the process of identifying, prioritizing, testing, deploying, and monitoring patches to address known vulnerabilities and keep systems up-to-date. The Company's patch management framework includes maintaining inventories of critical assets, prioritizing patching efforts based on technical or business characteristics, and deploying patches in a timely manner to minimize the window of opportunity for exploitation. Automated patching and regular monitoring of patch status are employed by the Company to ensure ongoing secure system configuration.
- In addition to patch management, the Company conducts routine system hardening which involves implementing various measures to enhance security and protect against potential threats, reducing the attack surface by disabling unused ports, accounts, or services. The patching and updating operating systems, removal of unnecessary applications and services, and correct configuration of user authentication.
- The Company maintains an inventory of software and licenses, ensuring lawful licensing.
- Access control in security involves identifying, authenticating, and authorizing individuals or systems to access resources, minimizing the risk of unauthorized access. Key aspects of the Company's access control framework include user account management, strong authentication methods (e.g., MFA), formal access request and approval processes, and periodic access reviews. Role-Based Access Control (RBAC) is the model used by the Company for managing permissions. For physical access, all Company premises require authentication from all individuals to be granted access.
- Protecting data in transit and at rest is a critical component of information security. ISO 27001 and NIST guidelines emphasize the use of strong encryption standards. For data in transit, the company uses the TLS 1.2+ protocol with strong ciphers. For data at rest the company is implementing full disk encryption (FDE), file-level encryption, and database encryption are employed holistically. The Company has also implemented proper key management (secure generation, storage, rotation, and destruction), to avoid weak key generation or hardcoded keys.
- A comprehensive backup and restore strategy is crucial for data protection and business continuity. The Company conducts backup procedures aligned with Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each system. These regular backups are done as a proactive measure for incident recovery. Backups are also encrypted both at rest and in transit, and access to

backup storage is restricted and requires secure authentication methods to gain access. Regular testing of restoration procedures is also carried out to ensure their reliability.

- Effective incident reporting is a core component of incident management. The Company's incident response lifecycle includes a "Detection and Analysis" stage, which emphasizes continuous monitoring and alerts, incident identification and validation, and classifying and prioritizing incidents. The Company has clear and communicated channels for staff to report anomalies. Incident reporting, escalation, containment, forensic evidence preservation, and recovery processes are all documented and kept on file by the Company and communicated accordingly.
- Root cause analysis (RCA) is a critical post-incident activity aimed at determining the fundamental reasons behind an incident to prevent recurrence. The Company's incident response lifecycle includes a "Post-Incident Activity" stage, where RCA is performed to identify underlying vulnerabilities, inadequate training, or human error that contributed to the incident. The Company is committed to efficient root cause analysis as part of its incident management and response system. This process helps the Company learn from incidents, evaluate the effectiveness of its response, and implement any identified improvements to its security posture.
- All outsourced services that process Company data will be subject to due diligence, documented risk assessment and a written contract that specifies security controls, audit rights, incident notification timelines, data handling limitations and termination requirements. Vendor risk is always assessed prior to onboarding and periodically thereafter.

4.3 Principle 3 — Maintain ongoing risk assessment program

Policy requirement: A standardized, documented risk management methodology will be used for asset inventory, threat/vulnerability identification, business impact analysis and risk treatment (accept/mitigate/avoid/transfer). Risk assessments shall be performed for new systems, major changes and periodically per the risk tiering.

- A risk register is a critical tool for documenting and managing identified risks within an organization. The Company is committed to the establishment and maintenance of a risk register as part of its information security risk assessment process. This register details each identified risk, its owner, a description of the risk, the likelihood and impact, the current risk level, planned mitigation actions, and the residual risk.
- The frequency of risk re-assessment is crucial for maintaining an effective information security management system. The Company will reconduct its risk assessments annually or whenever there are significant changes to the organizational mission, business processes, information systems, or operating environment, whichever occurs first.
- The Company will use standardized assessment report templates to ensure consistent and comprehensive documentation of risk assessments. Structured reporting helps to ensure that risk assessment results are clearly communicated to relevant stakeholders. These reports include an executive summary, a description of

the assessment scope and methodology, identified risks and their characteristics, risk ratings, recommended mitigation actions, and assumptions and limitations. Risk assessment reports, supporting evidence, and approvals are retained accordingly.

- For each identified risk the Company will record: owner, likelihood, impact, rating, selected treatment (mitigate / accept / avoid / transfer), remediation plan, target dates and residual risk. Risk assessment reports shall be reviewed by the ISM Coordinator and submitted to Senior Management for approval for any high and critical risks which cannot be mitigated or avoided.
- A Business Impact Assessment (BIA) process identifies and evaluates the potential effects of disruptions to business operations and information systems. The process employed by the Company involves identifying critical business functions, the resources that support them, and the maximum tolerable downtime (MTD) and recovery time objectives (RTO) for each. This allows the Company to prioritize recovery efforts and allocate resources effectively, informing both risk treatment and disaster recovery planning in the event of an incident occurring.

4.4 Principle 4 — Establish information security monitoring

Policy requirement: Implement continuous monitoring covering centralized log collection & analysis, capacity/performance monitoring, vulnerability management (patching, AV, IDS/IPS), and defined metrics (KPI/KGI). Logging and retention periods shall be risk-based..

- Security Information and Event Management (SIEM) configuration is critical for effective security monitoring and threat detection. The company has a purpose-built SIEM process that involves centralizing logs from various sources (e.g., network devices, servers, applications, API gateways), implementing methods of correlation to identify suspicious activities, and establishing real-time visibility. The process is also subjected to regular testing and tunings to minimize false positives and enhance detection capabilities.
- A well-defined retention policy is essential for managing information assets, meeting legal and regulatory obligations, and optimizing storage resources. The Company manages records in a manner which ensures they are protected from loss, destruction, falsification, unauthorized access, and unauthorized release. A comprehensive retention procedure is in place to specify the types of data to be retained, the duration of retention based on legal, regulatory, and business requirements, and secure disposal procedures. This procedure is communicated to all relevant personnel and regularly reviewed for compliance and effectiveness.
- Establishing appropriate incident alert thresholds is vital for timely detection and response to security incidents. The Company defines clear criteria for what constitutes an incident and when alerts should be triggered. These alert thresholds are risk-based, considering the criticality of the asset, the potential impact of an event, and the organization's risk appetite. Regular review and adjustment of these thresholds is conducted to adapt to evolving threat landscapes and improve the accuracy of alerts.
- Vulnerability scanning is an automated process of identifying security weaknesses in systems, applications, and networks. The Company will employ regular vulnerability

assessments to proactively identify and address security flaws. These regular vulnerability scans will help the Company maintain an up-to-date understanding of its security posture. The results of vulnerability scans will be analyzed, prioritized based on risk, and remediated in a timely manner, heavily integrated with the patch management and system hardening processes.

- Penetration testing is a simulated cyberattack against an information system to identify vulnerabilities that an attacker could exploit. Industry best practices encourage regular testing of security controls, and pentesting is a key method for this. The Company will contract independent, qualified individuals or teams of penetration testers to cover critical systems and applications, and include various attack vectors (e.g., network, web application, social engineering). The findings from these tests will be documented, prioritized, and used to remediate vulnerabilities and improve the overall security posture.

4.5 Principle 5 — Incident management & response

Policy requirement: Maintain documented incident reporting, escalation, containment, forensic evidence preservation, recovery and root cause processes. Maintain an incident register with records retained for minimum five years. Define communications (internal, clients, regulators) and disaster recovery activation criteria.

- Robust incident response procedures are essential for effectively managing and mitigating the impact of security incidents. The Company will employ documented incident management procedures, including reporting, assessment, response, and learning from incidents. The Company's internal incident management and response procedures clearly define roles and responsibilities, communication protocols, and steps for handling various types of incidents, ensuring a coordinated and efficient response.
- Clearly defined contact persons are crucial for efficient communication and coordination during a security incident. The Company has an incident response team with clearly assigned roles and contact information. This includes all relevant internal stakeholders (e.g., IT, legal, HR, management) as well as external parties where this may be required by law (e.g., law enforcement, regulatory bodies, customers, vendors).
- An incident register database is a centralized repository for documenting all security incidents, enabling effective tracking, analysis, and continuous improvement. The Company will maintain an incident register to record details such as the incident type, date and time, affected systems, impact, actions taken, and lessons learned. This database serves as a valuable resource for trend analysis, identifying recurring vulnerabilities, measuring the effectiveness of incident response efforts, and supporting post-incident reviews and audits.

4.6 Principle 6 — Privacy of customer information

Policy requirement: Protect the confidentiality and integrity of all client and provider data processed via our platform. Use data classification, least privilege, encryption in transit and

at rest where appropriate, contract clauses with clients/providers that define permitted uses, and a strict prohibition on selling or re-using data outside agreed purposes. Where personal data is processed, comply with applicable legal/regulatory privacy obligations and notify clients of processing activities.

- A data inventory is a comprehensive catalog of an organization's data assets, including their location, type, sensitivity, ownership, and lifecycle. The Company will maintain accurate and up-to-date inventories. These robust data inventories help the Company understand what data it possesses, where it resides, who is responsible for it, and what regulations apply, which is fundamental for effective data protection, risk management, and compliance with privacy laws like GDPR or CCPA.
- Data Loss Prevention (DLP) refers to technologies and processes designed to prevent sensitive information from leaving an organization's control. The Company will employ sufficient controls, in line with best practises, related to information flow enforcement. This involves identifying, monitoring, and protecting sensitive data across various channels (e.g., email, cloud storage, endpoints) to prevent unauthorized disclosure, exfiltration, or misuse. This helps facilitate a clear understanding of data classification, robust policies, and continuous monitoring and enforcement.
- As previously mentioned in earlier sections, encryption standards are established protocols and algorithms used to secure data, ensuring its confidentiality and integrity. The Company will use secure cryptographic controls to protect the confidentiality, authenticity, and integrity of information. The Company follows cryptographic best practices, including approved algorithms (e.g., AES for symmetric encryption, RSA or ECC for asymmetric encryption) and key lengths. Adhering to recognized encryption standards is crucial for protecting data both in transit (e.g., TLS 1.2+) and at rest (e.g., full disk encryption, file-level encryption), and for maintaining compliance with various regulatory requirements.
- Retention schedules dictate how long specific types of data must be kept and when they can be securely disposed of. The Company emphasizes the importance of managing records to ensure they are protected from loss, destruction, falsification, unauthorized access, and unauthorized release. The Company has a well-defined retention schedule based on legal, regulatory, and business requirements, helping the Company minimize storage costs, reduce legal risks, and ensure compliance with data protection and privacy regulations.
- Third-party data processing agreements are legally binding contracts that define the terms and conditions under which a third-party vendor processes data on behalf of an organization. The Company prioritizes the importance of managing risks associated with external providers, where applicable. These agreements will outline data protection responsibilities, security measures, audit rights, incident notification procedures, and compliance with relevant data protection laws (e.g., GDPR, CCPA). They are crucial for ensuring that sensitive data remains protected when handled by external entities and for maintaining accountability in the data supply chain.

4.7 Principle 7 — Information security training

Policy requirement: Provide security awareness training to all staff and long-term contractors within six months of joining and at least every three years thereafter; role-based training for staff with specific security duties. Training curriculum shall cover policies, threats, clean desk, access security, incident reporting and privacy.

- An effective information security training program is fundamental for cultivating a security-aware workforce. The Company will ensure that all relevant personnel receive appropriate information security awareness, education, and training. The Company will utilize a Learning Management System (LMS) to deliver and track training modules, which is sourced externally, to address specific organizational risks. The Company also maintains accurate completion registers, which is essential for demonstrating compliance and identifying training gaps. Onboarding checklists include mandatory security awareness training for all relevant new employees and long-term contractors. The Company will also conduct ongoing awareness training, such as phishing exercises, webinars, and regular security communications, as this is crucial to reinforce best practices and keep personnel informed about evolving threats.

4.8 Principle 8 — Audit the ISM program and process

Policy requirement: Implement periodic internal and independent external audits of ISM controls and program effectiveness. Audit scope, schedule and follow-up remediation tracking shall be documented and reported to the Board.

- The frequency and scope of audits are critical for ensuring the ongoing effectiveness of an Information Security Management (ISM) program. The Company will conduct internal audits at planned intervals and defines the audit criteria and scope for each audit. Audit frequency is determined by the organization's risk assessment, regulatory requirements, and any significant changes to the business or IT environment. The scope clearly defines what systems, processes, and controls will be examined, ensuring comprehensive coverage of the ISM framework.
- Effective remediation efforts and clearly assigned owners are essential for addressing audit findings and improving the security posture. The Company will take action to address nonconformities and their consequences, and to continually improve the suitability, adequacy, and effectiveness of the ISM. Each remediation effort has a designated owner responsible for its implementation, tracking progress, and reporting on its completion. This ensures accountability and timely resolution of identified weaknesses.
- Maintaining organized evidence repositories for audit document provision is crucial for demonstrating compliance and facilitating efficient audits. The Company will maintain documented information as evidence of the implementation of its audit program and the audit results. An evidence repository securely stores all relevant documentation, such as policies, procedures, risk assessments, audit reports, training records, and system configurations. This ensures that auditors can easily access the necessary information to verify control effectiveness and compliance with standards.

5. Definitions

Definitions used in this Policy adopt the Centrale Bank's glossary of definitions.

6. Policy maintenance & review

This Policy will be reviewed annually or sooner if significant changes occur to the business, legal/regulatory environment, or as a result of significant incidents. The ISM Representative will coordinate reviews and present changes to the Board for approval.